UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

CAPITOL RECORDS INC.; SONY BMG MUSIC ENTERTAINMENT; ARISTA RECORDS LLC; INTERSCOPE RECORDS; WARNER BROS. RECORDS INC.; and **UMG RECORDINGS INC.**, *Plaintiffs*, v. **JAMMIE THOMAS**, *Defendants*.	Case No. 06-cv-1497 (MJD/RLE) JURY DEMANDED

MEMORANDUM OF LAW IN SUPPORT OF

DEFENDANT'S MOTION TO SUPPRESS EVIDENCE

K.A.D. Camara
Camara & Sibley LLP
2339 University Boulevard
Houston, Texas 77005
713 893 7973
713-583-1131 (fax)
camara@camarasibley.com

Garrett Blanchfield
Brant D. Penney
Reinhardt, Wendorf & Blanchfield
332 Minnesota Street, Suite E-1250
St. Paul, Minnesota 55101
651-287-2100
651-287-2103
g.blanchfield@rwblawfirm.com

Attorneys for Defendant Jammie Thomas

Dated: June 1, 2009

TABLE OF CONTENTS

Table of Authorities

INTRODUCTION

I. MediaSentry Collected its Evidence Against Jammie Thomas in Violation of Federal and State Criminal Law

A. The Evidence Against Jammie Thomas

B. Minnesota Private Detectives Act

1. MediaSentry violated the Detectives Act

C. Federal Electronic Communications Statutes

1. Pen Register and Trap and Trace Devices Act, as amended by the USA Patriot Act

2. Electronic Communications Privacy Act of 1986

a. MediaSentry violated the Act

b. MediaSentry does not fall within any exception

II. This Court Can and, in the Interest of Justice and Deterrence, Should Suppress the Illegally Obtained Evidence Against Jammie Thomas

III. Conclusion

TABLE OF AUTHORITIES

FEDERAL CASES

Aiken v. Business and Industry Health Group, Inc.,
885 F. Supp. 1474 (D. Kan. 1995) 15, 17

Bell Atlantic Corp. v. Bolger,
2 F.3d 1304 (3d Cir. 1993) 15

Boyd v. United States,
116 U.S. 616 (1886) 19

Gelbard v. United States,
408 U.S. 41 (1972) 14

Konop v. Hawaiian Airlines, Inc.,
302 F.3d 868 (9th Cir. 2002) 14

In re U.S. for Orders (1) Authorizing Use of Pen Registers and Trap and Trace Devices,
515 F. Supp. 2d 325 9

U.S. v. Councilman,
418 F.3d 67 (1st Cir. 2005) 3

United States v. Carriger,
41 F.2d 545 (8th Cir. 1976) 14

United States v. Herring,
933 F.2d 932 (11th Cir.1991) 15

STATE CASES

Lake v. Wal-Mart Stores, Inc.,
582 N.W.2d 231 (Minn. 1998) 12

O'Brien v. O'Brien,
899 So. 2d 1133 (Fla.App. 5 Dist. 2005) 11, 18

State v. Ford,
539 N.W.2d 214 (Minn. 1995) 18

State v. Horner,
617 N.W.2d 789 (Minn. 2000) 7, 18

DOCKETED CASES

UMG Recordings Inc. v. Lindor,
No. 05-cv-1095 17

FEDERAL STATUTES

18 U.S.C. § 2511(1) 10, 11,12, 15

18 U.S.C. § 3121(a) 8

18 U.S.C. §3127(3) 8

147 Cong. Rec. S10990, S11000 (Oct. 25, 2001) 9

Cf. 18 U.S.C. § 2510(14) 10, 14

S. Rep. 99-541, 1986 U.S.C.C.A.N. 3555, 3590 (1986) 12

S. Rep. No. 1097, 90th Cong., 2d Sess., 66 (1968), *reprinted in* 1968
U.S.C.C.A.N. 2112, 2153 14

STATE STATUTES

Minn. Stat. §326.3341(4) 6

Minn. Stat. §326.339 6

Minn. Stat. §§626A.04, 626A.11 18

Minn. Stat. § 326.3341 6

Minn. Stat. § 326.338(2)-(4), (8) 5

Minn. Stat. § 629.37 7

Minnesota Private Detectives Act, Minn. Stat. § 326.338 *et seq* 5

TABLE OF EXHIBITS

Ex. A Private Investigators Licensed in Minnesota

Ex. B "MediaSentry Removes Investigative Language"

Ex. C Investigations of MediaSentry in Other States

Ex. D Senate Testimony Regarding Inadvertent File Sharing

Ex. E Examples of Inadvertent File Sharing

Ex. F KaZaA End User License Agreement (February 2005)

Ex. G Buckles Declaration

INTRODUCTION

The recording industry's only evidence that Jammie Thomas ever downloaded or shared music on KaZaA is the evidence that MediaSentry collected. MediaSentry collected this evidence in violation of federal and state criminal statutes that prohibit wiretapping and require that private investigators be properly trained and licensed. It collected this evidence at the direction and under the supervision of lawyers for the recording industry, including opposing counsel in this case. These same lawyers have used MediaSentry evidence to fuel not only this prosecution, but also their entire five-year campaign against tens of thousands of individuals accused of sharing music online — a litigation campaign that has earned their recording-industry clients more than $100 million in settlements.

In orchestrating this campaign, built around illegally obtained evidence and targeted at individuals, most of whom faced millions of dollars of potential liability without the assistance of counsel, these lawyers, led by Matthew Oppenheim and Richard Gabriel, violated the ethical rules governing our profession on an unprecedented scale. We respectfully request that this Court remedy this violation by suppressing all MediaSentry evidence in this case. We submit that, in this case, the first in which the recording industry's litigation campaign will be put on trial, the federal courts should make clear to the world that the kind of gross abuse of federal process that we have seen in the last seven years will never again be permitted.

If this Court grants our motion to suppress, we anticipate moving for a directed verdict for Jammie Thomas on all claims.

I. MEDIASENTRY COLLECTED ITS EVIDENCE AGAINST JAMMIE THOMAS IN VIOLATION OF FEDERAL AND STATE CRIMINAL LAW.

MediaSentry collected the evidence against Jammie Thomas in violation of the Minnesota Private Detective Act and the federal Pen Register and Trap and Trace Devices Act and Electronic Communications Privacy Act of 1986. These violations were crimes under Minnesota law and federal law.

A. The Evidence Against Jammie Thomas

The only evidence that Jammie Thomas downloaded or distributed music online is the dossier compiled by MediaSentry about Jammie's alleged use of KaZaA and the testimony of its representative, Mark Weaver.[1]

The RIAA and MediaSentry have utilized KaZaA to seek out and identify users who share copyrighted sound recordings. KaZaA is a peer-to-peer file sharing program used by millions of people worldwide to share files. KaZaA is actually one of a family of programs that interconnect using a peer-to-peer technology known as FastTrack. Peer-to-peer file sharing systems, including those based on FastTrack, allow a user to search for files that are available from other users of the system, and to selectively download files that are found as a result of this search.

The MediaSentry investigation typically proceeds as follows. MediaSentry, using its own copy of KaZaa, searches the KaZaA network for files with names that suggest sound recordings for which the recording companies own or hold license to the copyrights. When

[1] Most of this evidence is inadmissible for other reasons under the Federal Rules of Evidence. By describing this evidence here, we do not waive our objections submitted now or that we may raise at trial.

MediaSentry finds these files, they connect to the KaZaa instance running on the machine that is offering these files for download. Through the KaZaA interface, MediaSentry then lists all the files available on the remote machine. The KaZaA interface displays information about each file available. MediaSentry records an image for each screen displayed by KaZaA when it lists the available files. Finally, MediaSentry, using KaZaA, downloads selected files to their own machine to confirm that the files are in fact copyrighted sound recordings.

While running KaZaA, MediaSentry also utilizes a separate process (or computer program) to capture every packet of information that is sent between their instance of KaZaA and any other remote instance of KaZaA. In effect, MediaSentry monitors or taps into the network traffic between its instance of KaZaA and other instances of KaZaA. 1 Trial Tr. 185:2–5 ("We have a program that looks at the traffic that's coming in and grabs the relevant packets and logs them into a text file such as you see here.") This eavesdropping provides additional information to MediaSentry.

Information on the Internet is exchanged in discrete chunks called 'packets.' *U.S. v. Councilman* 418 F.3d 67 (1st Cir. 2005) (describing delivery of packets in context of email system). Like a mailing envelope, each packet has a sender and a recipient address. These addresses are in a special format consisting of four numbers (e.g. 128.0.0.1) and are known as IPv4 ("IP"), or Internet Protocol Version 4, addresses. *See* http://www.iana.org/numbers/. Many also compare IP addresses to phone numbers. 1 Trial Tr. 171:21 ("it's [the IP address] like a phone number on the Internet").

MediaSentry, through its eavesdropping software, captures every packet transferred including both the content of the packet, as well as the IP address of the source of the content 1 Trial Tr. 187:25 – 188:13 ("then there's the date, the source IP address…[a]nd then what would happen after this would be the actual song itself"). Through this process, unknown to the other parties communicated with over the internet, MediaSentry is able to determine the IP addresses of other KaZaA users machines. These IP addresses are then used in the subpoena process to determine the names and addresses of persons who are associated with the accounts to which the IP addresses were assigned on the dates and times of intercept by MediaSentry.

MediaSentry found Jammie by (1) using KaZaA to request a file transfer from Jammie's computer to a MediaSentry computer; (2) using a separate program or programs to intercept the Internet packets being sent from Jammie's computer to the MediaSentry computer as a result of this request; (3) reading the IP address of Jammie's computer from these packets; and (4) tracing this IP address back to Jammie. This kind of investigation of network traffic is lawful only after certain procedures are followed: when there is prior approval by a court and when the person conducting the investigation is properly licensed. When these procedures are not followed, such investigation constitutes criminal wiretapping and the illegal collection of evidence by an unlicensed private investigator.

B. Minnesota Private Detectives Act

1. MediaSentry violated the Detectives Act

MediaSentry collected evidence in violation of the Minnesota Private Detectives Act, Minn. Stat. § 326.338 *et seq*. MediaSentry violated § 326.3381 of the Detectives Act: "No person shall engage in the business of private detective . . . or advertise or indicate in any verbal statement or in written material that the person is so engaged or available to supply those services, without having first obtained a license." MediaSentry has never had a private-investigator license in Minnesota or any other state. *See* Ex. A (official listing of Minnesota-licensed private investigators).

MediaSentry violated § 326.3381 by engaging in the business of a private detective in Minnesota without a license. A person engages in the business of a private detective if "for a fee, reward, or other consideration" and "for the purpose of obtaining information for others" that person does any of nine listed acts, including:

- "investigating the identity, habits, conduct, movements, whereabouts, transactions, reputation, or character of any person";
- "investigating the credibility of witnesses or other persons";
- "investigating the location . . . of lost or stolen property"; or
- "obtaining through investigation evidence to be used . . . in preparation for trial of civil or criminal cases."

Minn. Stat. § 326.338(2)–(4), (8). MediaSentry did these things when it investigated the identity of the user of the computer from which it downloaded the songs here at issue (the user that the RIAA alleges is Jammie Thomas) and when it obtained, through its investigation, evidence of copyrighted songs on Jammie's computer.

MediaSentry also violated § 326.3381 by holding itself out to be a private detective and a supplier of private-detective services without a license. On its web site, MediaSentry described its services as "Investigation Services" and claimed "extensive experience gathering evidence for civil/criminal litigation and prosecution against those who engage in unauthorized online content distribution." Ex. B. It removed this information only in February 2008 as part of its defense against allegations by states attorney general that it was violating licensing acts like Minnesota's. *See, e.g.,* Ex. C (Maine, Massachusetts, Michigan, North Carolina, Oregon).

MediaSentry's violations were crimes under Minnesota law. *See* Minn. Stat. § 326.339 ("Unless otherwise specifically provided, any violation of any provision or requirement of sections 326.32 to 326.339 is a gross misdemeanor."). Although there are a variety of exemptions from the Detectives Act in Minn. Stat. § 326.3341, none of these exemptions apply. The closest is an exemption for "an investigator employed exclusively by an attorney or a law firm engaged in investigating legal matters." Minn. Stat. § 326.3341(4). This exemption does not apply because MediaSentry was not a law firm; MediaSentry was engaged by the RIAA, not the RIAA's attorneys; and MediaSentry and its employees did not work exclusively for the RIAA.

The policies underlying licensing statutes for private investigators have particular application in the context of peer-to-peer file-sharing networks like KaZaA. Inadvertent file sharing on these networks is common. Professor Eric Johnson of Dartmouth, in a recent study presented to the House Committee on Oversight and Government Reform, found sensitive medical records, social security numbers, and other personal information — files that no user would have shared intentionally — available from users' computers on peer-to-peer networks. *See* Ex. D (testimony).

Congress has launched investigations into the possible national-security consequences of inadvertent file sharing after a series of high-profile leaks of confidential documents. The leaked documents include the blueprints and avionics for Marine One, the President's helicopter; more than 150,000 tax returns, 25,800 student-loan applications, 626,000 credit reports, and the investment file of Justice Stephen Breyer. *See* Ex. E (news articles).

Licensing statutes like the Detective Act are an important tool of state law for preventing unauthorized persons from accessing inadvertently shared information like this. They represent a decision by the state that citizens' interest in privacy is more important than their interest in being able to engage companies like MediaSentry to detect private wrongs or even public crimes. Although private citizens may be privileged to arrest other citizens when they witness wrongdoing, they are not permitted to investigate potential wrongdoing without a license to do so. *See State v. Horner*, 617 N.W.2d 789, 794 (Minn. 2000).

Moreover, as the Minnesota Supreme Court explained in *Horner*, the proper remedy for an unauthorized investigation is suppression of any resulting evidence. *See id.* at 795 ("We therefore hold that citizens are not authorized to conduct investigations after observing a public offense committed in the citizen's presence under Minn. Stat. § 629.37. As such, even if the special deputies are considered private citizens, the district court properly excluded the results of both the field sobriety and preliminary breath tests.").

C. Federal Electronic Communications Statutes

MediaSentry's activities also constitute criminal violations of two federal statutes: (1) the Pen Register and Trap and Trace Devices Act, as amended by the USA PATRIOT Act (the "Pen Register Act"); and (2) the Electronic Communications Privacy Act of 1986 (the "Wiretap Act"). The TCP/IP packets that MediaSentry intercepted contained both recipient and sender IP addresses and the actual contents of the file being transferred over the Internet. The Pen Register Act makes it a crime to record IP addresses, while the Wiretap Act makes it a crime to examine the contents of the IP packets as they cross the Internet. Further, the screen captures by MediaSentry were interceptions of electronic communications and also violated the Wiretap Act.

1. Pen Register and Trap and Trace Devices Act, as amended by the USA PATRIOT Act

MediaSentry violated the Pen Register Act when they recorded the TCP/IP packets that included the IP address of the sender. It is a misdemeanor under 18 U.S.C. § 3121(a) to install or use a pen register or trap and trace device. In 2001, the Pen Register Act was amended to broaden the definition of "pen register" to any "device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication." 18 U.S.C. § 3127(3)

Importantly, the definition of pen register has not been read to exclude address-recording devices that also record content, but instead the definition has been read to prohibit court orders allowing the use of pen registers that also collect content. *In re U.S. for Orders (1) Authorizing Use of Pen Registers and Trap and Trace Devices*, 515 F.Supp.2d 325 E.D.N.Y., 2007, *citing* 147 Cong. Rec. S10990, *S11000 (Oct. 25, 2001) ("When I added the direction on use of reasonably available technology ... to the pen register statute as part of [CALEA] in 1994, I recognized that these devices collected content and that such collection was unconstitutional on the mere relevance standard.”). Thus, MediaSentry’s software that records the IP addresses of senders violates the Pen Register Act.

2. Electronic Communications Privacy Act of 1986

a. MediaSentry violated the Act

MediaSentry’s activities violated the Electronic Communications Privacy Act of 1986 (the “Wiretap Act”), the federal statute that prohibits unauthorized wiretapping. The Wiretap Act broadly prohibits wiretapping:

> Except as otherwise specifically provided in this chapter, any person who —
>
> (a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;
>
> .* * *
>
> (c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; [or]
>
> (d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection,
>
> shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

18 U.S.C. § 2511(1).

MediaSentry violated 18 § 2511(1)(A) by intercepting electronic communications, namely, the packets traveling between the KaZaA clients on Jammie’s computer and

MediaSentry's computer. The Wiretap Act defines *intercept* as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4). As Weaver testified at the last trial, this interception was done intentionally and at the behest of counsel for the RIAA:

> Weaver: "And then we use the Kazaa application to actually download a sample of the songs that the user is distributing. And while we're doing that, we'll also — we have a program which monitors the traffic going back and forth.
>
> And so when that process is finished, we just combine all of those things up into a bundle of data that we then pass onto the record companies. And that's basically a capture or a capture report.
>
> Gabriel: You just used the phrase "monitors traffic." Could you describe —
>
> Weaver: When I use the term "traffic," I'm talking about the data that goes back and forth over the Internet. So whenever I, for example, were to download a file, the file has to get to me, so it will be streaming to me. And that's what I mean when I say "traffic."

1 Trial Tr. 156:5–156:20. MediaSentry's "monitoring" of traffic constitutes the interception of an electronic communication.

When MediaSentry recorded images of the KaZaA interface they further violated § 2511(1)(A). The display screen interface of KaZaA constituted an electronic communication from the sender to the MediaSentry operator. In this case the screen communicated information about the files on the sender's computer. When MediaSentry recorded the image of the screen they "intercepted" these electronic communications. *O'Brien v. O'Brien,* 899 So.2d 1133 (Fla.App. 5 Dist. 2005) (recorded screenshots constitute interception of electronic communications)

b. MediaSentry does not fall within any exception

MediaSentry does not fall within any of the exceptions to the Wiretap Act. The exceptions that come closest to applying are those in 18 U.S.C. § 2511(2)(d) and 18 U.S.C. § 2511(2)(g)(1). Section 2511(2)(d) provides:

> It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.

18 U.S.C. § 2511(2)(d). This section permits interception of an electronic communication where one party to the communication, here, MediaSentry, consents, but only if the interception is not done "for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State." *Id.*

Section 2511(2)(d) does not protect MediaSentry because MediaSentry was intercepting communications for the purpose of committing the crime under Minnesota law of engaging in the business of a private detective without a license and the crime under federal law of recording IP addresses in violation of the Pen Register Act. We also note that Minnesota recognizes the tort of intrusion upon seclusion where one "intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns . . . if the intrusion would be highly offensive to a reasonable person." *Lake v. Wal-Mart Stores, Inc.*, 582 N.W.2d 231, 233 (Minn. 1998) (citing Restatement (2d) of Torts § 652B (1977)). The kind of unauthorized, unlicensed hacking that MediaSentry engaged in would be highly offensive to a reasonable person and is therefore tortious in addition to criminal.

MediaSentry also does not qualify for the exception in § 2511(2)(g)(i). That section provides:

> It shall not be unlawful under this chapter or chapter 121 of this title for any person — (i) to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public

18 U.S.C. § 2511(2)(g)(i). This section does not apply because the KaZaA network is available only to users of KaZaA who consent to certain terms of use, not to the general public. Further, KaZaA encrypts the information it sends between different nodes, and that information is not generally visible or available to the public. Thus, the electronic communications over the KaZaA network that MediaSentry monitored were not "readily accessible to the general public."

The Senate Report accompanying enactment of § 2511(2)(g)(i) explains that whether an electronic communication is readily accessible depends on whether the public is freely authorized to access the electronic communication. *See* S. Rep. 99-541, 1986 U.S.C.C.A.N. 3555, 3590 (1986). It explains that a service is generally accessible if it "does not require any special access code or warning to indicate that the information is private." KaZaA requires both these things: it requires a username and password to log on to the network and decode the encrypted communications, and such a username and password can be obtained only by signing on to certain terms of use that give notice that the electronic communications on the network are private.

The KaZaA terms of use forbid exactly what MediaSentry did in this case: (1) making requests to gather information about other users; (2) storing information about other users; (3) violating state and federal laws; (4) developing and deploying separate software to monitor the network; and (5) altering data stored by KaZaA on MediaSentry's computer. Specifically, MediaSentry violated the following terms:

> 2.11 [What You Can't Do Under This License] Monitor traffic or make search requests in order to accumulate information about individual users;
>
> 2.14 [What You Can't Do Under This License] Collect or store personal data or other information about other users;
>
> 2.9 [What You Can't Do Under This License] Interfere with or disrupt the Software;
>
> 2.10 [What You Can't Do Under This License] Intentionally or unintentionally violate any applicable local, state, national or international law, including securities exchange and any regulations requirements, procedures or policies in force from time to time relating to the Software;
>
> 3.4 You may not use, test or otherwise utilize the Software in any manner for purposes of developing or implementing any method or application that is intended to monitor or interfere with the functioning of the Software.
>
> 3.5 You may not through the use of any third party software application, alter or modify the values stored by the Software in your computer's memory, on your computer's hard disk, or in your computer's registry, or, with the exception of completely uninstalling the Software, otherwise modify, alter or block the functioning of the Software.

See Ex. F (KaZaA End User License Agreement, February 2005).

These terms of use, violated by MediaSentry, show that KaZaA was not a network containing electronic communications generally accessible to the public, but was instead a private network for communications between users who had obtained special usernames and passwords and who consented to certain restrictive terms and conditions. *See Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 875 (9th Cir. 2002) ("Congress wanted to protect electronic communications that are configured to be private."). Moreover, KaZaA encrypts communications on its network to preserve privacy. *Cf.* 18 U.S.C. § 2510(14) (encrypted radio communications are not readily accessible to the public). Just as a locked door creates an expectation of privacy, *see United States v. Carriger*, 41 F.2d 545 (8th Cir. 1976), the steps that KaZaA took to protect electronic communications on the KaZaA network make tapping into those communications without authorization an example of criminal wiretapping.

The Supreme Court has observed that the Wiretap Act has as its dual purpose (1) protecting the privacy of wire and oral communications, and (2) delineating on a uniform basis the circumstances and conditions under which the interception of wire and oral communications may be authorized. *Gelbard v. United States*, 408 U.S. 41, 48 (1972) (citing S. Rep. No. 1097, 90th Cong., 2d Sess., 66 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2153). The Court also noted that: "[a]lthough Title III authorizes invasions of individual privacy under certain circumstances, the protection of privacy was an overriding congressional concern." *Id.* In 1986, Congress amended Title III to include electronic communications, with the idea in mind that the wiretap laws had to be updated in order to take into account new telecommunication technologies. *See United States v. Herring*, 933 F.2d 932, 935 (11th Cir.1991).

Because no exceptions to the Wiretap Act's prohibition on interception of electronic communications apply, the interception that MediaSentry used to gather the evidence now deployed against Jammie Thomas in this case constituted a criminal violation of the Wiretap Act. *See* 18 U.S.C. § 2511(4)(a).

II. THIS COURT CAN AND, IN THE INTEREST OF JUSTICE AND DETERRENCE, SHOULD SUPPRESS THE ILLEGALLY OBTAINED EVIDENCE AGAINST JAMMIE THOMAS

A federal court has power to suppress illegally obtained evidence when that evidence was obtained at the direction and under the supervision of lawyers in violation of their ethical obligations. *Aiken v. Business and Industry Health Group, Inc.*, 885 F. Supp. 1474, 1480 n.7 (D. Kan. 1995) ("Strict adherence to these rules is demanded and any information gained in violation of an applicable ethical guideline remains subject to suppression."). "The ethical standards imposed upon attorneys in federal court are a matter of federal law. We look to the Model Rules of Professional Conduct to furnish the appropriate ethical standard." *Bell Atlantic Corp. v. Bolger*, 2 F.3d 1304, 1316 (3d Cir. 1993).

The Model Rules of Professional Conduct forbid "methods of obtaining evidence that violate the legal rights of . . . a [third] person." Rule 4.4. The methods of obtaining evidence employed by MediaSentry violated the legal rights of Jammie Thomas under the Private Detectives Act, the Pen Register Act, and the Wiretap Act, as described in Part I, *supra*. *Cf.* ABA Formal Opinion 01-422: Electronic Recordings by Lawyers (holding, in the context of voice recordings, that violation of state wiretap laws is violation of rules of professional conduct). In all respects relevant to this case, the Minnesota Rules of Professional Conduct, the Colorado Rules of Professional Conduct, and the ethical rules of most other states mirror the Model Rules.

The Model Rules make lawyers responsible for misconduct by persons whom they are supervising when the lawyer approves the conduct or learns of the conduct in time to avoid or mitigate its consequences:

> With respect to a nonlawyer employed or retained by or associated with a lawyer: . . .
>
> (c) a lawyer shall be responsible for conduct of such a person that would be a violation of the Rules of Professional Conduct if engaged in by a lawyer if:
>
> > (1) the lawyer orders or, with the knowledge of the specific conduct, ratifies the conduct involved; or
> >
> > (2) the lawyer is a partner or has comparable managerial authority in the law firm in which the person is employed, or has direct supervisory authority over the person, and knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action.

Rule 5.3.

The lawyers who orchestrated the RIAA's litigation campaign were ethically responsible for the conduct of MediaSentry, their "investigative arm." These lawyers knew or should have known that MediaSentry's activities were illegal at latest when MediaSentry began receiving notice from states that its actions were in violation of state private detective and wiretapping laws – before the investigation of Jammie Thomas was initiated. *See* Ex. C. Moreover, these lawyers were intimately involved in crafting MediaSentry's investigative strategy and reviewing the dossiers that MediaSentry brought in.

In a declaration filed in *UMG Recordings Inc. v. Lindor*, No. 05-cv-1095 in the United States District Court for the Eastern District of New York, Bradley A. Buckles, the RIAA's Executive Vice President, Anti-Piracy, explained the close relationship between the RIAA's lawyers and MediaSentry. *See* Ex. G. Buckles declared:

> [T]he MediaSentry Agreement provides detailed information regarding the instructions and parameters for conducting on-line investigations that were discussed and developed by the RIAA and its counsel, on behalf of the RIAA's members. . . .
>
> As the detailed instructions and search parameters of the MediaSentry Agreement show, MediaSentry was intimately involved in the formulation of the legal strategy developed by the RIAA's anti-piracy team, including the record companies' counsel. This strategy formed the basis of the legal advice that was provided to the record companies regarding how best to investigate and capture infringers, and this legal advice, which I believe to be subject to the attorney-client privilege, is reflected in the MediaSentry Agreement. Moreover, the information contained in the MediaSentry Agreement and the Agreement itself were generated directly and exclusively because of potential litigation, and these documents reflect the mental impressions of counsel, particularly as to the record companies' and their counsel's strategy for enforcing the record companies' substantial copyright interests.

Ex. G. According to Buckles, MediaSentry was so deeply integrated with the RIAA's legal team that the privilege extends to the RIAA's engagement agreement with MediaSentry.

As a matter of federal substantive law, this Court has the inherent power to suppress evidence obtained in violation of the ethics rules that apply in federal court. *See Aiken*, 885 F. Supp. at 1480 n.7; *see also State v. Ford*, 539 N.W.2d 214 (Minn. 1995) (supervisory power includes power to suppress evidence); *O'Brien v. O'Brien*, 899 So. 2d 1133, 1137–38 (Fla. App. 2005) (suppressing evidence obtained in violation of the Wiretap Act and collecting cases on discretion of trial courts to suppress evidence). Exercising this discretion to suppress the MediaSentry evidence is particularly appropriate in this case because Minnesota law provides for suppression. *See Horner*, 617 N.W.2d at 795; Minn. Stat. §§ 626A.04, 626A.11 (inadmissibility of evidence obtained by illegal wiretap under state wiretap statute that parallels federal statute).

III. CONCLUSION

This is an unprecedented case. It is the first of the more than 30,000 prosecutions brought by the RIAA against those who download music online to go to trial. And it is one of only a handful of these prosecutions in which the defendant is vigorously challenging the RIAA's legal strategy. This case is also part of an unprecedented litigation campaign being waged by an entire industry, acting as one, with a single set of lawyers and a single investigative arm under a single statute for the single measure of statutory damages in the single forum of the federal courts — an unprecedented campaign in which the recording industry has threatened tens of thousands of individuals with millions of dollars of potential liability in order to extract settlements that now add up to well over $100 million for the recording industry and its lawyers.

We ask this Court to consider whether a litigation campaign like this, unique in the history of the federal courts, is appropriate. We submit that it is not. It is an unethical strategy created by lawyers to obtain evidence by criminal means and use this evidence to intimidate individuals, usually unrepresented by counsel, into settling so often that out of more than 30,000 defendants over seven years, Jammie Thomas is the first to take her case to trial. What drives this campaign is the illegal evidence that MediaSentry collects. What would end it is suppression of that evidence.

A final point: Although the law regarding civil statutory damages in non-commercial copyright infringement cases remains a topic of vigorous debate, an oft-missed point is that excessive damages may have the effect of rendering a civil statute quasi-criminal in nature. The *Boyd* holding is still valid these many years later. *Boyd v. United States,* 116 U.S. 616, 634 (1886) ("As, therefore, suits for penalties and forfeitures, incurred by the commission of offenses against the law, are of this quasi criminal nature, we think that they are within the reason of criminal proceedings for all the purposes of the fourth amendment of the constitution, and of that portion of the fifth amendment which declares that no person shall be compelled in any criminal case to be a witness against himself").

Where the penalties, as in this case, are almost entirely punitive, there is a heightened need for protection of defendants right to a fair and just trial, without threat of prosecution with unlawfully obtained evidence. This Court, without needing to reach the issue as a matter of constitutional law, may take judicial notice of the penalties faced by Jammie Thomas when reaching a discretionary decision about suppression of evidence gathered in violation of state and federal laws — especially where such laws were enacted specifically to protect the privacy of citizens.

Respectfully submitted,

/s/ K.A.D. Camara

K.A.D. Camara
Camara & Sibley LLP
2339 University Boulevard
Houston, Texas 77005
713 893 7973
713-583-1131 (fax)
camara@camarasibley.com

Garrett Blanchfield, #209855
Brant D. Penney, #0316878
Reinhardt, Wendorf & Blanchfield
332 Minnesota Street, Suite E-1250
St. Paul, Minnesota 55101
651-287-2100
651-287-2103

g.blanchfield@rwblawfirm.com

Attorneys for Defendant Jammie Thomas

Dated: June 1, 2009